



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

09/838,123

04/20/2001

Noel D. Matchett

000505

8687

38834

7590

02/09/2005

WESTERMAN, HATTORI, DANIELS & ADRIAN, LLP
1250 CONNECTICUT AVENUE, NW
SUITE 700
WASHINGTON, DC 20036

EXAMINER

LEMMA, SAMSON B

ART UNIT

PAPER NUMBER

2132

DATE MAILED: 02/09/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/838,123	Applicant(s) MATCHETT ET AL.	
	Examiner Samson B Lemma	Art Unit 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 20 April 2001.
2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 13-31 is/are pending in the application.
4a) Of the above claim(s) _____ is/are withdrawn from consideration.
5) ☐ Claim(s) _____ is/are allowed.
6) ☒ Claim(s) 13-31 is/are rejected.
7) ☐ Claim(s) _____ is/are objected to.
8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. **Claims 13-31** have been examined.

Preliminary Amendment

2. The preliminary amendment, submitted and requested for consideration by the applicant is acknowledged. The office action has been written after the submitted preliminary amendment is taken in to account.

3. **Claims 1-12** have been cancelled and new **claims 13-31** have been added by the applicant. Only the new **claims 13-31** are examined.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

5. **Claims 13-20 and 23-31** are rejected under 35 U.S.C. 103(a) as being unpatentable over Thomas J. Roberts (hereinafter referred as **Roberts**) (U.S. Patent No 5,008,935) in view of the Michael C. Wood (hereinafter referred as **Wood**) (U.S. Patent No 5,003,596)

Art Unit: 2132

6. **As per claim 13,25-27 and 31 Roberts discloses** in a device for performing the **Data Encryption Standard (DES) on a block of data bits under control of a DES key,** [Abstract] (the blocks are encrypted under the control of a first key using any block encryption method such as the Data Encryption Standard DES) **the combination with a modified "P" permutation in the "f function.**[Abstract] (individual bytes of the encrypted blocks of a buffer are then permuted under the control of a second key to form an encrypted buffer)

Roberts does not expressly disclose

- The modified permutation "P / or the variable permutation "P is actually inside the "f function of the encryption device in the encryption process.

However, in the same field of endeavor, Wood discloses that variable permutation which is connected to S-box permutation under the control of the key in the encryption process.[See figure 8, ref. Num "106"; ref. Num "134" and ref. Num "116" and column 4, lines 51-52]

It would have been obvious to one having ordinary skill in the art at the time the invention was made to replace the fixed permutation of the conventional DES with the variable permutation of the as per teachings of **Wood** and combine it into the method taught by **Roberts** in order to strengthen the security of data encryption process of DES.

7. **As per claims 14,** the combinations of **Roberts and Wood** discloses the improved device as applied to claim 13, above. Furthermore **Roberts** discloses the improved device includes a second cipher key to specify said modified "P" permutation. .[Abstract] (individual bytes of the encrypted blocks of a buffer are then permuted under the control of a second key to form an encrypted buffer)

Art Unit: 2132

8. As per claims 15, the combinations of **Roberts and Wood** discloses the improved device as applied to claim 13, above. Furthermore **Wood** discloses the improved device includes a logic gates for implementing said modified "P" permutation.[Page 16]
9. As per claims 16-20 , 23 and 29, the combinations of **Roberts and Wood** discloses the improved device as applied to claim 13 and 27, above. Furthermore **Wood** discloses the improved device wherein said modified "P" permutation is selected by a control signal. [Fig 8, ref. Num "116"] (the control signal is the key form the key table memory as shown on figure 8, ref. Num "116") .
10. As per claims 24, the combinations of **Roberts and Wood** discloses the improved device as applied to claim 13, above. Furthermore **Roberts** discloses the improved device wherein including said first key and a second cipher key.[column 1, lines 54-63]
11. As per claims 28, the combinations of **Roberts and Wood** discloses the improved device as applied to claim 27, above. Furthermore **Roberts** discloses the improved device wherein the modified permutation is dependent upon a second cipher key. [column 1, lines 54-63; Abstract]
12. As per claims 30, the combinations of **Roberts and Wood** discloses the improved device as applied to claim 13, above. Furthermore **Wood** discloses the improved device wherein said modified permutation is a function of a subset of said first key and a second cipher key. [column 1, lines 54-63; Abstract]
13. Claims 21-22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Thomas J. Roberts (hereinafter referred as **Roberts**) (U.S. Patent No 5,008,935) in view of the Michael C. Wood (hereinafter referred as **Wood**) (U.S. Patent No 5,003,596) further in view of the publication paper by **Michael Portz**, title "On the Use of Interconnection Network in Cryptography ".(hereinafter referred as **Portz**) (Publication 1991) (reference U)

Art Unit: 2132

14. As per claims 21-22, the combinations of **Roberts and Wood** discloses the improved device as applied to claim 15, above. Furthermore **Wood** discloses the improved device includes a logic gates for implementing said modified "P" permutation.[Page 16]
The combination of **Roberts and Wood** does not expressly disclose said logic gates comprise a Benes-Waksman network.
However, in the same field of endeavor, **Portz** discloses logic gates comprise of a Benes-Waksman network.[figure 5]
It would have been obvious to one having ordinary skill in the art at the time the invention was made to combine Benes-Waksman network, which is used as the logic gates as per teachings of **Portz** into the method taught by by the combination of **Roberts and Wood** in order to add the cryptography advantage of the Interconnection network.[see **Portz**, paragraph 1, lines 1-5]

Conclusion

15. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.(See PTO-Form 892).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Samson B Lemma whose telephone number is 571-272-3806. The examiner can normally be reached on Monday-Friday (8:00 am---4: 30 pm). If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, BARRON JR GILBERTO can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status

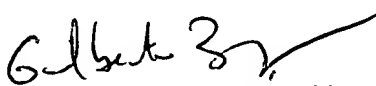
Art Unit: 2132

information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

SAMSON LEMMA

S.L

02/02/2005


GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100